How to submit a code review that uses custom rules

This page has been made public for vendors

Question

I scanned our application using a custom rulepack. What information should be included with the V&V Secure Code Review package?

Answer

When a custom rulepack is used in the scan of an application, the VA Secure Code Review SOP requires that the developers include the custom rulepack(s) in the materials provided for review. As part of the review, each of the rules in the rulepack will be examined to ensure that the rule is appropriate and does not remove true positive findings from the scan results, which will in those cases result in scan issues being reported in V&V secure code review validation reports.

A custom Fortify rule definition by itself usually does not provide enough information for the reviewer to determine whether or not it is appropriate so the developers should provide additional information about the rule. Some information that is useful to provide:

- The category (e.g., Privacy Violation) of the findings that the rule affects
- Examples of findings in that category that were affected (could be file name and line number of some of the findings that were removed)
- Why these findings should be removed - same type of information that would be provided when auditing the findings

There are several ways to provide this information. More documentation and information is better than less in this case. Any combination of the following may be provided:

- A rule may be annotated with notes that provide the additional information
- The information may be provided in a separate document
- A scan of the application that does **not** use the custom rulepack(s) may be provided along with the scan that does use them. This can be used to illustrate the category and findings that were eliminated by the custom rules. This additional scan does not need to be audited. If a second scan is used, please include a readme file that indicates the purpose of the alternate scan file so there is no confusion.

If not enough information is provided to determine whether or not a rule is appropriate, it will be reported as a scan issue in the report which will result in a failure for the review.

References

- VA Secure Code Review SOP

HPE Fortify Version	4.40 and later
Programming Language	☐ C/C++ ☐ .NET ☐ Java ☐ Objective -C ☐ Other
Fortify Audit Workbench	☐ Yes ☐ No
Fortify IDE Plugin	☐ Yes ☐ No
Other Fortify Component	☐ Yes ☐ No

Request code review tools, validations, and support HERE.